IN THE CLAIMS:

1.-31. (Cancelled)

32. (New) An authentication communication method comprising:

transmitting scrambled access information from an access apparatus to a storage medium, the scrambled access information generated by scrambling access information, the access information including information designating an area in the storage medium used for storing digital information;

authenticating, in the access apparatus, whether the storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information;

authenticating, in the storage medium, whether the access apparatus is authorized according to a challenge-response authentication protocol without using the scrambled access information; and

reading/writing the digital information from/into the area designated by the access information after the storage medium and the access apparatus have authenticated each other as authorized devices.

33. (New) An authentication communication method according to claim 32, wherein:

said authenticating, in the access apparatus, whether the storage medium is authorized according to the challenge-response authentication protocol includes comparing a first response value and a second response value;

said first response value is calculated in the storage medium using the scrambled access information; and

said second response value is calculated in the access apparatus using the scrambled access information.

34. (New) An authentication communication method according to claim 32,

wherein the access information includes information designating an address and a size of the area of the storage medium.

35. (New) An authentication communication system comprising: a storage medium; and

an access apparatus operable to read/write digital information from/into the storage medium;

said storage medium comprising:

an area for storing the digital information; and

a first authentication unit operable to authenticate whether the access apparatus is authorized according to a challenge-response authentication protocol without using scrambled access information; and

said access apparatus comprising:

a transmitting unit operable to transmit the scrambled access information to said storage medium, the scrambled access information generated by scrambling access information, the access information including information designating an area in said storage medium used for storing digital information;

a second authentication unit operable to authenticate whether said storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information; and

an accessing unit operable to read/write the digital information from/into the area designated by the access information after said storage medium and said access apparatus have authenticated each other as authorized devices.

36. (New) An authentication communication system according to claim 35, wherein:

said first authentication unit is operable to calculate a first response value using the scrambled access information and send the first response value to said second authentication unit of said access apparatus;

said second authentication unit is operable to calculate a second response value using the scrambled access information; and

said second authentication unit is operable to authenticate whether said storage medium is authorized according to the challenge-response authentication protocol in which the first response value and the second response value are compared.

37. (New) An authentication communication system according to claim 35,

wherein the access information includes information designating an address and a size of the area included in the storage medium.

38. (New) An authentication communication program stored in a computer-readable storage medium, said program comprising:

a transmitting program code operable to transmit scrambled access information from an access apparatus to a storage medium, the scrambled access information generated by scrambling access information, the access information including information designating an area in the storage medium used for storing digital information;

a first authenticating program code operable to authenticate whether the storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information;

a second authenticating program code operable to authenticate whether the access apparatus is authorized according to a challenge-response authentication protocol without using the scrambled access information; and

a reading/writing program code operable to read/write the digital information from/into the area designated by the access information after the storage medium and the access apparatus have authenticated each other as authorized devices.